

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
WESTERN DISTRICT

FILED
JUL 05 2018

Matthew Thibault
CLERK

CR 5:18-mj-88

IN THE MATTER OF THE SEARCH OF:
The premises known as the offices of
Dropbox, Inc., located at 333 Brannan
St., San Francisco, CA, 94107, for the
account associated with user Jessica
Smith and account
js2842675@gmail.com

**AFFIDAVIT IN SUPPORT OF
SEARCH WARRANT
APPLICATION**

State of South Dakota)
) ss
County of Pennington)

INTRODUCTION AND AGENT BACKGROUND

1. I, Brian Freeouf, Investigator with the Pennington County Sheriff's Office (PCSO) and currently assigned to the South Dakota Internet Crimes Against Children Taskforce (ICAC), being duly sworn, states as follows:

2. I began my law enforcement career with Pennington County in July of 2005. I spent approximately 3 years on patrol in the contract community of Wall, SD. I was then assigned to the patrol division in Rapid City in 2008. I was promoted to the rank of Senior Deputy in July of 2010. I also spent time as a School Liaison Officer and Criminal Investigations Division as a Property Crimes Investigator. Even though I was assigned as a Property Crimes Investigator I also investigated other crimes including, but not limited to, homicides, rapes, assaults, and coroner duties. My other assignments within the Sheriff's Office include Deputy Coroner, Field Training Deputy, and Defensive Tactics Training Administrator. Due to the placement on ICAC, I have also been given the title of

Special Assistant Attorney General of the State of South Dakota.

3. I have investigated and assisted in the investigation of cases involving the possession, receipt, and distribution of child pornography in violation of federal law to include United States Statutes 18 U.S.C. §§ 2251, 2252 and 2252A, involving violations of law involving child pornography and 18 U.S.C. § 2422(b), enticement of a minor using the internet. During my law enforcement career, I have become familiar with the *modus operandi* of persons involved in the illegal production, distribution and possession of child pornography and those who engage in enticement of minors using the internet. Based on my experience and training, I am knowledgeable of the various means utilized by individuals who illegally produce, distribute, receive and possess child pornography.

4. I have been informed that 18 U.S.C. §§ 2251, 2252 and 2252A prohibit the manufacture, distribution, receipt and possession of child pornography and that 18 U.S.C. § 2422(b), prohibits enticing a minor to produce child pornography using the internet.

5. The facts set forth in this affidavit are based on my personal knowledge, knowledge obtained from other individuals, including other law enforcement officers, interviews of persons with knowledge, my review of documents, interview reports and computer records related to this investigation, communications with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience. This affidavit contains information necessary to support

probable cause for this application and does not contain every material fact that I have learned during the course of this investigation; however, I have not withheld information known to me that would tend to negate probable cause has been withheld from this affidavit.

ITEMS TO BE SEARCHED FOR AND SEIZED:

6. This affidavit is submitted in support of an application for a search warrant for the contents of and information pertaining to a drop box account found during the investigation of Kyle Soto, which is more specifically described in Attachment A, for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251, 2252, and 2252A (production, receipt and possession of child pornography), and 18 U.S.C. § 2422(b), enticement of a minor using the internet. The items are more specifically described in Attachment B. The Dropbox, Inc. account is associated with email: js2842675@gmail.com (also referred to in this affidavit as "Target Account") from the date the user opened the Dropbox Inc. account to the date of this search warrant.

DEFINITIONS

7. The following definitions apply to this Affidavit and Attachments A and B:

a. "Chat," as used herein, refers to any kind of text communication transmitted over the Internet in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format, that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as

Internet forums and email.

b. “Chat room”, as used herein, refers to the ability of individuals to meet in one location on the Internet in order to communicate electronically in real-time to other individuals. Individuals may also have the ability to transmit electronic files to other individuals within the chat room.

c. “Child Erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

d. “Child pornography,” as defined in 18 U.S.C. § 2256(8), is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

e. “Cloud-based storage service,” as used herein, refers to a publically accessible, online storage provider that collectors of child pornography can use to store and trade child pornography in larger volumes. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography in order to grant access to their collections. Such services allow individuals to access these files easily through a wide variety of electronic

devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to file stored on a cloud-based service does not need to be a user of the service to access the file. Access is free and readily available to anyone who has an internet connection.

f. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones and devices. See 18 U.S.C. § 1030(e)(1).

g. "Computer hardware," as used herein, consists of all equipment, which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

h. "Computer software," as used herein, is digital information, which a computer can interpret and any of its related components to direct the way they

work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

i. “Computer-related documentation,” as used herein, consists of written, recorded, printed, or electronically stored material, which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

j. “Computer passwords, pass-phrases and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alphanumeric characters) usually operates as a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

k. A provider of “Electronic Communication Service” (“ESP”), as defined in 18 U.S.C. § 2510(15), is any service that provides to users thereof the ability to send or receive wire or electronic communications. For example, “telephone companies and electronic mail companies” generally act as providers of electronic communication services. See S. Rep. No. 99-541 (1986), reprinted in

1986 U.S.C.C.A.N. 3555, 3568.

l. “Electronic Storage Device” includes but is not limited to external and internal hard drives, thumb drives, flash drives, SD cards, gaming devices with storage capability, storage discs (CDs and DVDs), cameras, cellular phones, smart phones and phones with photo-taking and/or internet access capabilities, and any “cloud” storage by any provider.

m. “File Transfer Protocol” (“FTP”), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

n. “Hyperlink” refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

o. “Hyper Text Markup Language”, or “HTML”, as used herein, is a standard protocol for formatting and displaying documents, such as web pages, on the Internet.

p. “Internet Protocol address” or “IP address,” as used herein, refers to a unique number used by a computer to access the Internet. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet.

q. “Internet Service Providers” (“ISPs”), as used herein, are commercial

organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

r. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

s. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

t. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

u. "Remote Computing Service" ("RCS"), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

v. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

w. "Short Message Service" ("SMS"), as used herein, is a service used

to send text messages to mobile phones. SMS is also often referred to as texting, sending text messages or text messaging. The service allows the user to send short text messages from one cell phone to another cell phone or from the Web to another cell phone. The term "computer," as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

x. "Storage medium" A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

y. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

**BACKGROUND ON CHILD EXPLOITATION AND CHILD PORNOGRAPHY,
COMPUTERS, THE INTERNET, EMAIL AND FILE SHARING SERVICES**

8. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. File sharing services, like Dropbox, Inc., are commonly utilized for both legitimate file sharing as well as illicit file sharing.

b. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers serve many functions for persons who exploit children online; they serve as a mechanism for meeting child-victims and communicate with them; they serve as a mechanism to get images of the children and send images of themselves; computers serve as the manner in which persons who exploit children online can meet one another and compare notes.

c. Persons, who exploit children online, can now transfer printed photographs into a computer-readable format with a device known as a scanner and then distribute the images using email, like Gmail and Yahoo! Inc. Furthermore, with the advent of digital cameras and smartphones with cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera or smartphone to the computer. In the last ten years, the resolution of pictures taken by digital cameras and smartphones has increased dramatically, meaning that such pictures have become sharper and crisper. Photos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can

save video footage in a digital format directly to a hard drive in the camera. The user can easily transfer video files from the camcorder to a computer.

d. A device known as a modem allows any computer to connect to another computer with telephone, cable, or wireless connection. People can make electronic contact to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Persons can transfer child pornography via electronic mail or through file transfer protocols (FTP's) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "instant messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

e. The Internet affords individuals several different venues for meeting and exploiting children in a relatively secure and anonymous fashion.

f. Individuals also use online resources to exploit children, including services offered by Internet Portals such as Gmail and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can

set up an online storage account from any computer with access to the Internet. Even in cases where a user utilizes online storage is, evidence of child pornography can be found on the user's computer or external media in most cases.

9. Based on my training and experience and investigation in this case, I have learned the following about Dropbox, Inc.:

- a. Dropbox is a file syncing and collaboration service that allows users to access and share their files on computers, phones, tablets and the Dropbox website.
- b. Each Dropbox account is associated with a single email address at any given point. If a user were to share login information for an account, more than one person could plausibly take actions in the Dropbox account at the same time, but would all appear as the same user to Dropbox.
- c. IP addresses of specific actions within a Dropbox account, such as uploads and deletions, are not available.
- d. IP address login information is recorded when a user logs in to Dropbox through Dropbox's website. Like many online services, Dropbox sometimes uses cookies stored on a browser so that a user may not need to sign in every time they visit the website. Additionally, if a user is accessing files in their Dropbox account from a desktop or mobile application, that access may not be logged by Dropbox.

- e. If a Dropbox user is a member of a shared folder, then other members of the shared folder can also upload content. Also, if a user shares their login information (email and password), then other people could login and upload files. Users can use the "file request" feature to receive files directly on their Dropbox from another person, even if that person does not have a Dropbox account.
- f. "Dropbox" refers to an online storage medium on the internet accessed from a computer or electronic storage device. As an example, online storage mediums such as Dropbox make it possible for the user to have access to saved files without the requirement of storing said files on their own computer or other electronic storage device. Dropbox is an "offsite" storage medium for data that can be viewed at any time from any device capable of accessing the internet. Users can store their files on Dropbox and avoid having the files appear on their computer. Anyone searching an individual's computer that utilizes Dropbox would not be able to view these files if the user opted only to store them at an offsite such as Dropbox. These are often viewed as advantageous for collectors of child pornography in that they can enjoy an added level of anonymity and security.
- g. Dropbox provides a variety of on-line services, including online storage access, to the general public. Dropbox allows subscribers

to obtain accounts at the domain name www.dropbox.com.

Subscribers obtain a Dropbox account by registering with an email address. During the registration process, Dropbox asks subscribers to provide basic personal identifying information. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

- h. When the subscriber transfers a file to a Dropbox account, it is initiated at the user's computer, transferred via the Internet to the Dropbox servers, and then can automatically be synchronized and transmitted to other computers or electronic devices that have been registered with that Dropbox account. This includes online storage in Dropbox servers. If the subscriber does not delete the content, the files can remain on Dropbox servers indefinitely. Even if the subscriber deletes their account, it may continue to be available on the Dropbox servers for a certain period of time.
- i. Online storage providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or

closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, online storage providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

- j. In some cases, Dropbox account users will communicate directly with Dropbox about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Online storage providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

10. From my training and experience, I am aware that Dropbox's computers contain information and other stored electronic communications belonging to unrelated third parties. Accordingly, this affidavit and application for search warrant seeks authorization solely to search the computer accounts and/or files for information and the content of communications pertaining to the Target Account specified herein and in Attachment A, following the procedures described herein.

PROBABLE CAUSE

11. On April 17, 2018, South Dakota ICAC Commander SSA Brent Gromer contacted me and advised me the Rhode Island ICAC needed assistance locating a suspect in South Dakota. SSA Gromer sent me the case information, including that Bristol Police Department Detective John Nappi was investigating the case. The case consisted of an 11yo boy being exploited online for naked images of himself. Detective Nappi developed an IP address being used by the suspect's email account. That IP address is registered to Midcontinent Communications out of Sioux Falls SD. Detective Nappi sent Midcontinent Communications a search warrant but they would not honor it due the fact it was not signed by a Federal Court or a Court from the state of South Dakota.

12. During the month of February 2018, Martha Finnegan, a Rhode Island resident, made a complaint with the Federal Bureau of Investigation (FBI) regarding an unknown individual soliciting child pornography from an 11 year-old male, for whom she is the legal guardian. The FBI referred this investigation to the Rhode Island State Police and the Rhode Island ICAC Task Force. In his affidavit, Nappi referred to the 11 year-old as "John Doe" to protect his identity.

13. On February 20, 2018, Nappi met with Martha Finnegan in regard to this complaint. Finnegan stated she is the legal guardian for 11 year-old John Doe. Finnegan stated she was going through John Doe's email and discovered that Doe had been conversing with an unknown male (suspect). The suspect offered to pay Doe to send an explicit video of himself. Doe had sent the suspect an image exhibiting his penis in a graphic and lascivious manner. The suspect

further stated he/she would share the illicit photograph of Doe with Doe's mother if Doe refused to send a video displaying his genitals. Doe's electronic devices were turned over to Nappi for forensic analysis. Finnegan provided consent for the RI ICAC to assume Doe's online identity in order to further this investigation.

14. Detective Lavalley, member of the ICAC Task Force, signed in to Doe's email utilizing the username and password provided by Finnegan. Nappi located an email conversation between Doe and the suspect, who was utilizing the email account, *shane118@gmail.com* with the user name *Shana Roberts*. It was apparent that Doe deleted his emails, therefore not all were visible. There were a number of sections of the conversation that were accessible by reading the threads attached to sent messages.

15. On November 15, 2017, the suspect extorted Doe and solicited Doe to produce and send child pornography. Below is an excerpt from the conversation, all chat conversations are verbatim, including misspellings and grammatical errors:

Doe: Give me the fucking money

Suspect: not till i get something since you left when i was gonna pay you

Suspect: last chance !

Suspect: ok well good thing i recorded you naked i will post it online so ur mom sees it.

Suspect: goodluck online...(juvenile victim's name omitted)

Later in the conversation:

Suspect: send me a full naked pic on here then and I will send it. because you left

Doe: ok

16. On February 20, 2018, Detective Lavallee began communicating with the suspect in an undercover capacity, portraying himself as the 11 year-old male. Detective Lavallee learned that at some unknown time, the victim and the suspect engaged in a video chat on the website Fruzo. During that video chat, the victim displayed his genitals on the video. The suspect took a screen shot of the video, which showed the victim with his genitals exposed. The suspect also alleged that he saved the entire video. During the conversation, the suspect solicited Detective Lavallee, a person he (the suspect) believed to be an 11 year-old male, to produce and send child pronography, stating he would pay Detective Lavallee for a video of child pornography. The suspect also attempted to extort Detective Lavallee. Below is an excerpt from the conversation:

Suspect: Last Chance. One video and ill pay

Undercover: sry im jst nervous. u kno im 11, if I get caught my mom will ground me til im 18 lol

Suspect: She won't find out when u sent it delete it from ur phone. U wont get caught

Undercover: y should I trust ull send the money

Suspect: Because im risking lots of money!! Im not gonna scam u

Suspect: Ok i went and bought a 200\$ card believe me now?? (The suspect included a photograph of an Amazon gift card)

Undercover: lol ur not risking ne thing lol. i send u a video then u don't send it and im screwed and u have my video and still have the money

Suspect: I just sent a picture of the card i bought. If you want the code send me a video

Undercover: right but it's the same thing, how do I know ull give me the code?

Suspect: I gave you proof....clearly you don't want it..

Undercover: I do im just scared

Suspect: No need to be...i wont show anyone and im rich I will pay you

Suspect: Here is half the code.... X7HS-9KD2. You will get the other half after the video

Undercover: im too scared

Suspect: You don't have to show your face.. nobody will know its you ok?

Undercover: so what do you want me to show then?

Suspect: Just you naked from your stomach down...and jacking off your dick

Undercover: idk

Suspect: Well guess what I recorded you that time we were on fruzo so if you don't want me to post this online and show ur mom...i need a video now

Suspect: Im not joking

Suspect: Then make a video now or im gonna show her.

Suspect: I know ur name so I can find her really easily. If we make a deal i wont show her tho

17. During the chat conversation, the suspect also sent Detective Lavallee child pornography in the form of an image of what the suspect alleged to be a screen shot of the aforementioned video chat on Fruzo. The image depicted a male, believed to be the victim, 11 year-old John Doe, displaying his genitals to the camera in a lude and lascivious manner.

18. On February 22, 2018, legal process was sent to Google Legal Investigations Support. On April 6, 2018 Google responded to the legal process. Nappi viewed the Internet Protocol (IP) connection logs associated with the Google email address *shane118@gmail.com*. The IP connection logs showed logins and logouts occurred from February 19, 2018 at 01:14:53 UTC to February 21, 2018 23:59:47. Nappi conducted an inquiry with the American Registry of Internet Numbers (ARIN) and determined that owner of IP address 208.107.164.178 was MidContinent Communications, 3901 N. Louise Avenue, Sioux Falls, South Dakota 57107.

19. Thereafter, I confirmed the IP address and it is assigned to Midcontinent Communications. I was also able to locate that IP address was being utilized in the Rapid City area market. This would indicate the user of the IP address likely lives in the Rapid City area.

20. On April 17, 2018, I applied for a search warrant reference user information of the IP address 208.107.164.178. The Honorable Judge Matt Brown granted the search warrant and I proceeded to serve that search warrant on Midcontinent Communications. Midcontinent Responded later that day with the following information:

Erica Soto
[REDACTED]

Rapid City, SD 57702

Home Phone: 605-545-2644

21. I checked if Erica was listed in our local law enforcement system and I did not find any information for her. I checked social media was able to find a Facebook account for Erica Soto who lives in Rapid City. Further examination showed she is married to Kyle Soto.

22. On April 17, 2018, at about 1500 hours, I drove past the Soto residence in Rapid City. The house faces south and is a single level home. The numbers [REDACTED] are visibly displayed on the front porch pillar of the home. The house has brown siding halfway up the house and is beige in color the rest of the way up. There was a black GMC Terrain sitting out front of the house. The vehicle was backed into the driveway and there was not a license plate on the front of the vehicle.

23. I communicated with Detective Nappi via email and I told him the information I had obtained. He told me based on the last name he had previously developed a suspect named Kyle Soto. I told him he appeared to be the husband to the Erica Soto. Detective Nappi agreed with me and sent me an image they had receive during their investigation of the suspect. The image provided to me of the man appeared to be the same person I saw on Erica Soto's Facebook and Kyle Soto's Facebook.

24. On April 19, 2018, I checked if Kyle Soto was listed in our local law enforcement system. Kyle was in our local system. In 2016, Kyle was the victim

of a vehicle burglary. At the time, Kyle was living at the Soto residence in Rapid City. The vehicle that was burglarized was a 2011 Black GMC Terrain, like the one I saw in the driveway, with Florida License Plate CNME22. In 2017, Kyle was also served civil paperwork at the Soto residence. Based on the Internet history, the car, and the photos of both Erica and Kyle being married. I believe Kyle Soto lives at [REDACTED], and was the individual commanding John Doe to engage in production of child pornography.

25. While preparing for the search warrant of the house, I stayed in contact with Detective Nappi and he advised me of the following. Detective Nappi had served a search warrant for the email account which was being utilized by Kyle Soto during the chats with the 11yo victim and the undercover officers. The email account is shane118@gmail.com. Detective Nappi advised he had also received the contents of the email from Gmail. They were able to find the video and chat of their 11yo victim. Further follow up is needed, but they found numerous other unidentified minor victims who were also enticed for naked images in the same manner as their 11yo victim.

26. Detective Nappi advised he believed this email was being utilized by Kyle Soto based on the IP address which came back to his residence is the same IP address used to log into the Gmail account. A photo which was captured from the chats of the suspect matched a photo of Kyle on Facebook.

27. Forensic Analyst Hollie Strand is in the process of conducting a forensic examination on several devices seized during the house search warrant. On Soto's phone, Strand has found over one hundred thumbnails of separate

chats with people appearing to be minors. Some of the chats included child pornography. In addition, Erica brought me several other devices, including a camera, which contained remnants of images of child pornography, which had been deleted from the device. In addition, Erica provided me a cellular phone, previously used by Soto, which also contained images of child pornography.

28. Detective Nappi provided me with the search warrant content he received regarding the shanel118@gmail.com account. I have begun to examine the content of the account. Within that account I have observed innumerable communications between Soto and other users. I observed the communications with the known victim from Rhode Island. In addition, I saw communications between Soto and a currently unidentified 15 year-old female who during the chats lamented that he was abusing her by continuously seeking images of child pornography, that he was a pedophile, and that she was engaging in self-harm due to his continued abuse. Soto's response was she needed to produce another video of child pornography or he would expose the previously provided images to social media and that she needed to "rub it faster," likely referring to her clitoris.

29. The Subject Account is associated with the shanel118@gmail.com account. When I interviewed Soto, he told me that the Subject Account is his primary email account. Erica Soto confirmed that the Subject Account is Soto's email account. I observed a photograph in the shanel118@gmail.com account in which the person photographed held up a sign stating "Lish 1586." There is another image of possible child pornography in the shanel118@gmail.com account in which "Lish 1586" is written on a bare breast with a visible nipple. I

know that persons engaged in online communications with strangers often have the other user "prove" he/she is not law enforcement by holding up signs related to the nature of their communications, dates, etc. I also would note that the Target Account Lish1586@gmail.com is similar to Kyle1586CK@yahoo.com, which is the recovery email address for the shanel18@gmail.com account. I would point out that images of child pornography were located on Soto's cellular phone and often cell phone users will access their primary email address from their cell phones. Therefore, there is probable cause to believe that Soto would utilize his primary email address via his cell phone, which may explain some of the child pornography contained on the phone. In addition, I commonly see that persons engaging in online exploitation of children will utilize multiple email addresses.

30. During my manual search of Soto's cell phone, I noticed the Dropbox app on the cell phone. I opened the app and the account information associated with that Dropbox app was username Jessica Smith and js2842675@gmail.com. I observed images of pornography, but due to the lack of internet connectivity based on the phone being in airplane mode, I could not connect to the images to enlarge them and determine if they are images of child pornography. During my exam of the phone's content, I noticed that on multiple occasions, Soto assumed the persona of a female, which could explain the use of a female's name on his Dropbox account.

31. Based on my training and experience I know that individuals who possess, manufacture, and distribute child pornography use multiple ways to

access, store and distribute it. I know that it is common for individuals who distribute child pornography to place these files into cloud databases such as One Drive and/or Dropbox, Inc. These individuals know that companies are monitoring user emails for this type of contraband. Individuals that distribute child pornography place these files into cloud databases and then share the links to these databases through emails. They know that the links will not trigger any alarms by the email companies such as Yahoo, Inc. or Google, Inc. (Gmail).

**CHARACTERISTICS COMMON TO INDIVIDUALS WHO HAVE A SEXUAL
INTEREST IN CHILDREN AND/OR WHO RECEIVE AND/OR POSSESS
CHILD PORNOGRAPHY**

32. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who have a sexual interest in children and/or receive, or possess images of child pornography:

- a. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.
- b. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs,

magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children often retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children and/or receive, or possess images of child pornography often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. The possessor typically keeps the child pornography close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images,

which are valued highly.

e. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography also may correspond with and/or meet others to share information and materials. These individuals rarely destroy correspondence from other child pornography distributors/possessors or conceal such correspondence as they do their sexually explicit material. They often maintain lists of names, addresses, and telephone numbers of individuals they have been in contact with who share the same interests in child pornography.

f. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography prefer not to be without their child pornography for any prolonged time-period. Law enforcement officers involved in the investigation of child pornography throughout the world have documented this behavior. Thus, even if the unknown user uses a portable device (such as a mobile cell phone) to access the internet and child pornography, it is more likely than not an examiner will find evidence of this access within the SUBJECT ACCOUNT.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

33. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Dropbox, Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Attachment A and Section

I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

JURISDICTION

34. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711(3). 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, this Court is a “district court of the United States (including a magistrate judge of such court)” that “has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

REQUEST/JUSTIFICATION FOR ORDER OF NONDISCLOSURE

35. The United States respectfully applies for an order of nondisclosure to Google, Inc. under 18 U.S.C. § 2705(b) regarding the Dropbox, Inc. account associated with email address js2842675@gmail.com. The United States is seeking this search warrant for subscriber information, including all names, addresses, IP addresses, including historical, telephone numbers, other email addresses, information on length and types of services and any means of payment related to these accounts under the authority given by 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A). Based on § 2703(c)(3), the United States is not required to provide notice to the subscriber. Under § 2705(b), the United States may apply to the court for an order commanding Dropbox, Inc. not to notify the subscriber of the existence of the search warrant. The court may decide what length of time shall apply to the order of nondisclosure if the court determines the notification to the subscriber could result in one of the five factors

listed in the statute, which includes destruction of or tampering with evidence. 18 U.S.C. § 2705(b)(3). The basis for the request is that such disclosure could cause any person with access to the accounts, or any related account or account information, to tamper with or modify the content or account information and thereby destroy or tamper with evidence and otherwise seriously jeopardize the investigation. Especially due to the ease of access to Dropbox, Inc., persons can modify its content with internet access and sufficient account information. As such, the United States respectfully requests this Court enter an order commanding Dropbox, Inc. not to notify the user of the existence of this warrant.

REQUEST FOR SEALING OF MATTER

36. I request that the Court order sealing this case until further order of the Court. The documents filed in the case discuss an ongoing criminal investigation that is neither public nor known to all the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

LIMIT ON SCOPE OF SEARCH

37. I submit that if during the search, agents find evidence of crimes not set forth in this affidavit, another agent or I will seek a separate warrant.

CONCLUSION

38. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on computer systems owned,

maintained, controlled and/or operated by Dropbox, Inc., contain evidence of crimes, contraband, instrumentalities, and/or fruits of violations of criminal laws as specified herein, including identification of the person who used the electronic accounts described in Attachment A. The facts outlined above show that the Dropbox, Inc. account, listed in Attachment A have been used for the exploitation of children using the internet including violations of 18 U.S.C. §§ 2252, 2252A (production, receipt and possession of child pornography), which items are more specifically described in Attachment B. There is probable cause to believe that the unidentified user of the Dropbox, Inc. account received and distributed child pornography with other unknown users and thereby violated the aforementioned statutes in the District of South Dakota and elsewhere. The account is the subject of this warrant affidavit. The accounts the Dropbox Inc. account associated with username Jessica Smith and email js2842675@gmail.com.

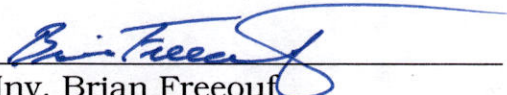
39. Law Enforcement agents will serve the warrant on Dropbox, Inc., who will then compile the requested records at a time convenient to it, so there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

40. For these reasons, I request authority to seize all electronic communications and other content stored in the Target Account, and for the Court to authorize search of the items seized in an off-site controlled environment. Law enforcement officers and agents will review the records sought

by the search warrant and will segregate any messages and content constituting evidence, fruits or instrumentalities of violations of federal criminal law. Additionally, I request authority to serve the warrant on Dropbox, Inc. via the internet and to allow Dropbox, Inc. to copy the data outside of this agent's presence.


RETURN COMPLIANCE BY DROPBOX, INC.

41. Dropbox's policies prohibit mailing or emailing child pornography to law enforcement in response to a search warrant, instead requiring a law enforcement officer to personally appear and collect contraband materials, unless the means of production is explicitly described in that search warrant. Specifically, Dropbox requires the Court order the disclosure, notwithstanding 18 U.S.C. § 2252A or similar statute or code.


Inv. Brian Freeouf
Pennington County Sheriff's Office
and Internet Crimes Against
Children Taskforce

SUBSCRIBED and SWORN to in my presence

this 5th day of July, 2018.


DANETA WOLLMANN
U.S. MAGISTRATE JUDGE